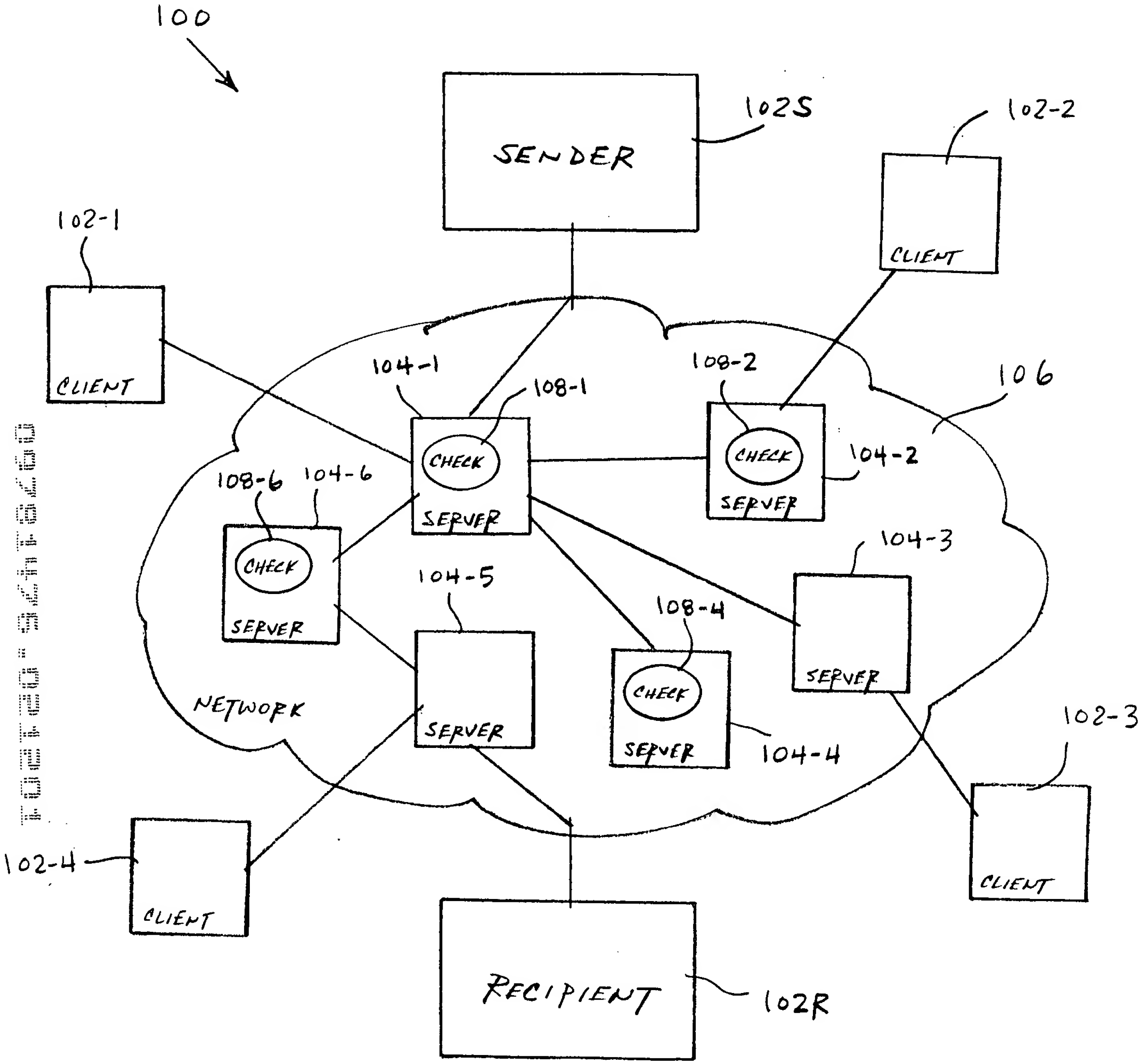
100
SENDER
102S
102-2
CLIENT
102-1
CLIENT
104-1
108-1
108-2
106
CHECK
SERVER
CHECK
SERVER
104-2
108-6
104-6
CHECK
SERVER
104-5
104-3
108-4
SERVER
CHECK
SERVER
NETWORK
SERVER
104-4
102-3
CLIENT
102-4
CLIENT
RECIPIENT
102R

FIG. 1

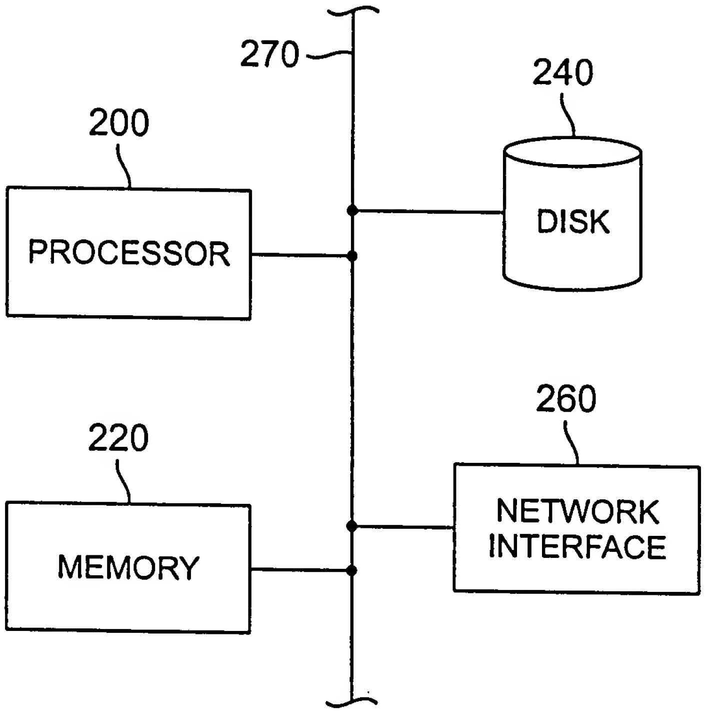
270
240
200
DISK
PROCESSOR
260
220
NETWORK INTERFACE
MEMORY

FIG. 2

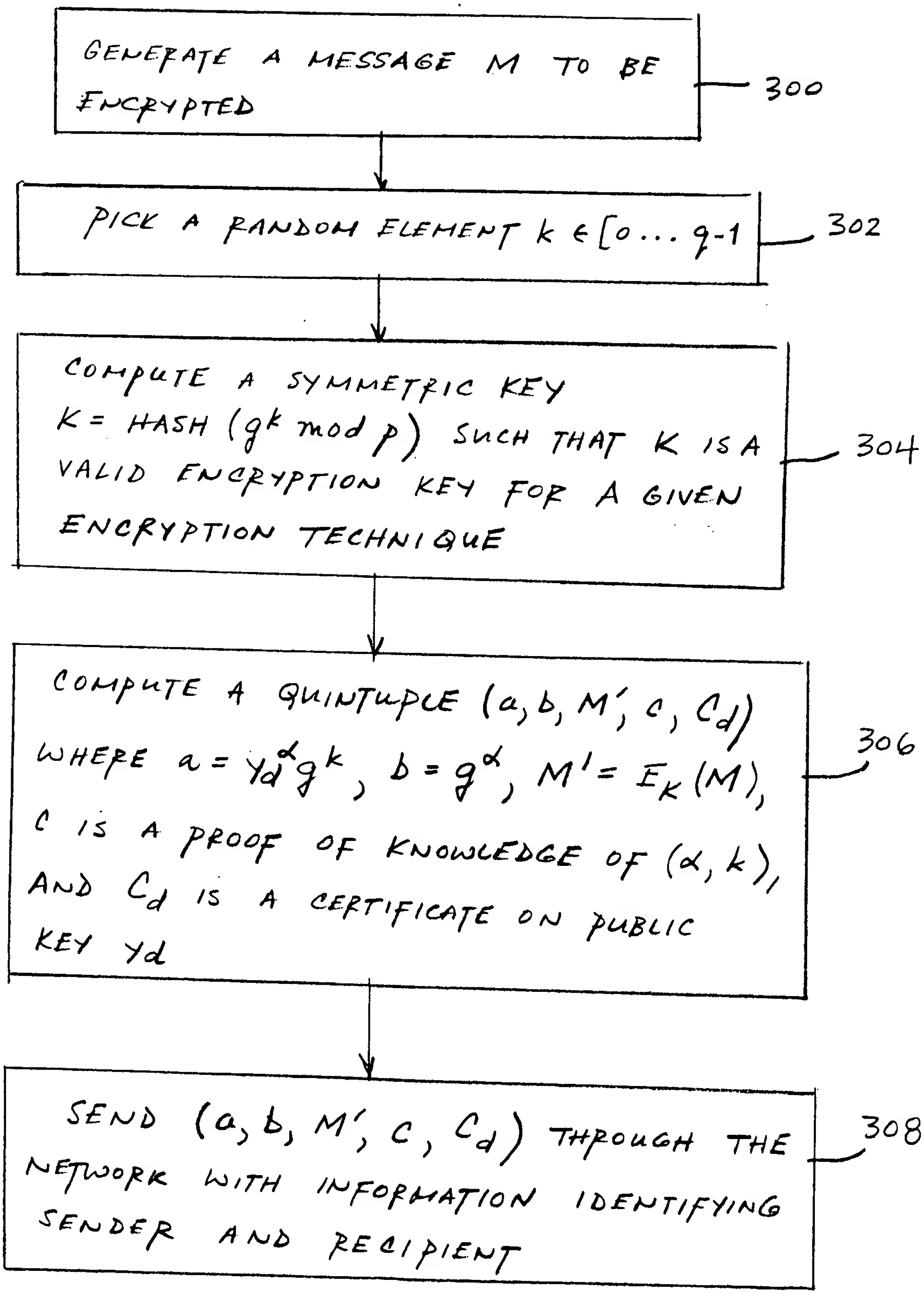
GENERATE A MESSAGE M TO BE ENCRYPTED
300
PICK A RANDOM ELEMENT $k \in [0 \ldots q-1$
302
COMPUTE A SYMMETRIC KEY $K = HASH(g^k \bmod p)$ SUCH THAT K IS A VALID ENCRYPTION KEY FOR A GIVEN ENCRYPTION TECHNIQUE
304
COMPUTE A QUINTUPLE (a, b, M', c, C_d) WHERE $a = y_d^{\alpha} g^k$, $b = g^{\alpha}$, $M' = E_K(M)$, c IS A PROOF OF KNOWLEDGE OF (α, k), AND C_d IS A CERTIFICATE ON PUBLIC KEY y_d
306
SEND (a, b, M', c, C_d) THROUGH THE NETWORK WITH INFORMATION IDENTIFYING SENDER AND RECIPIENT
308

FIG. 3

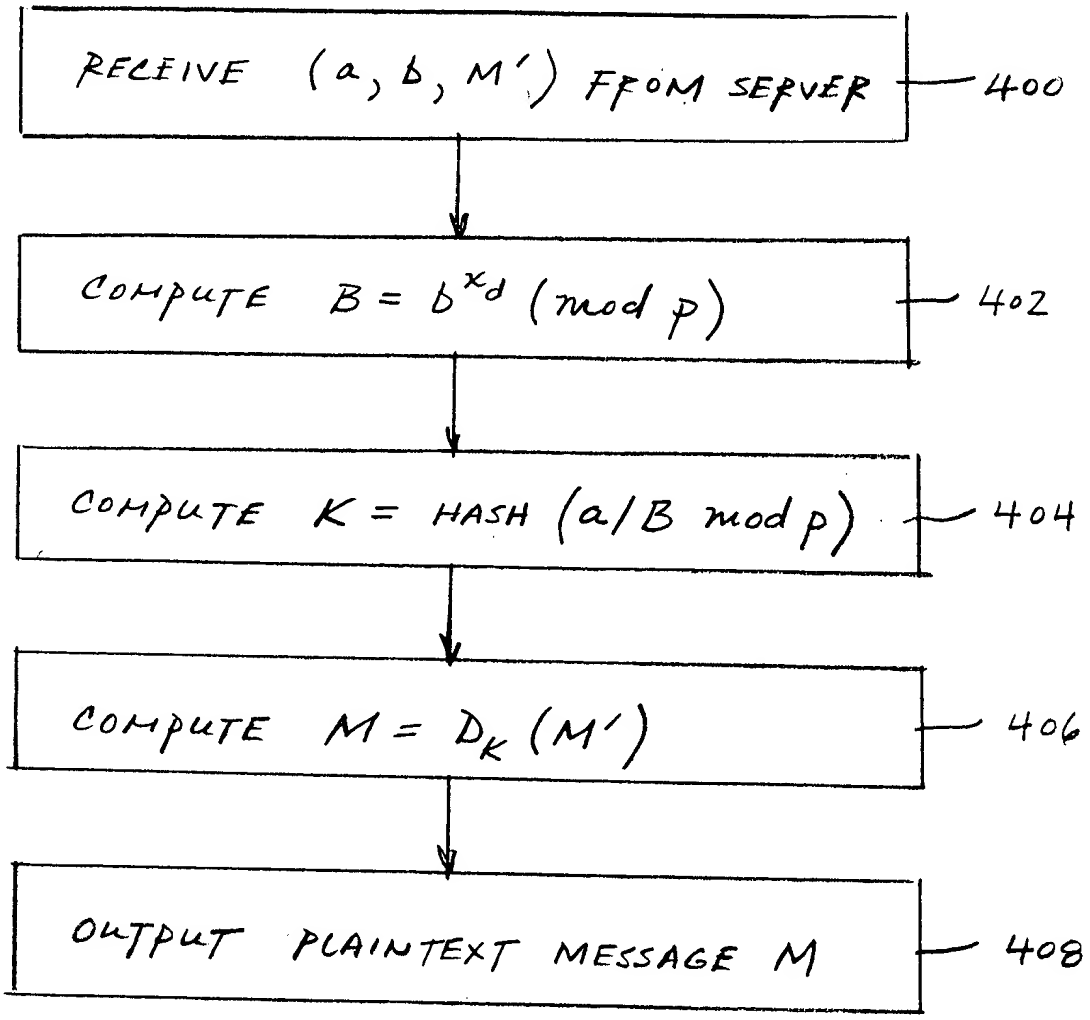
RECEIVE (a, b, M′) FROM SERVER
400
COMPUTE $B = b^{x_d} \pmod p$
402
COMPUTE $K = \text{HASH}(a/B \bmod p)$
404
COMPUTE $M = D_K(M')$
406
OUTPUT PLAINTEXT MESSAGE M
408

FIG. 4

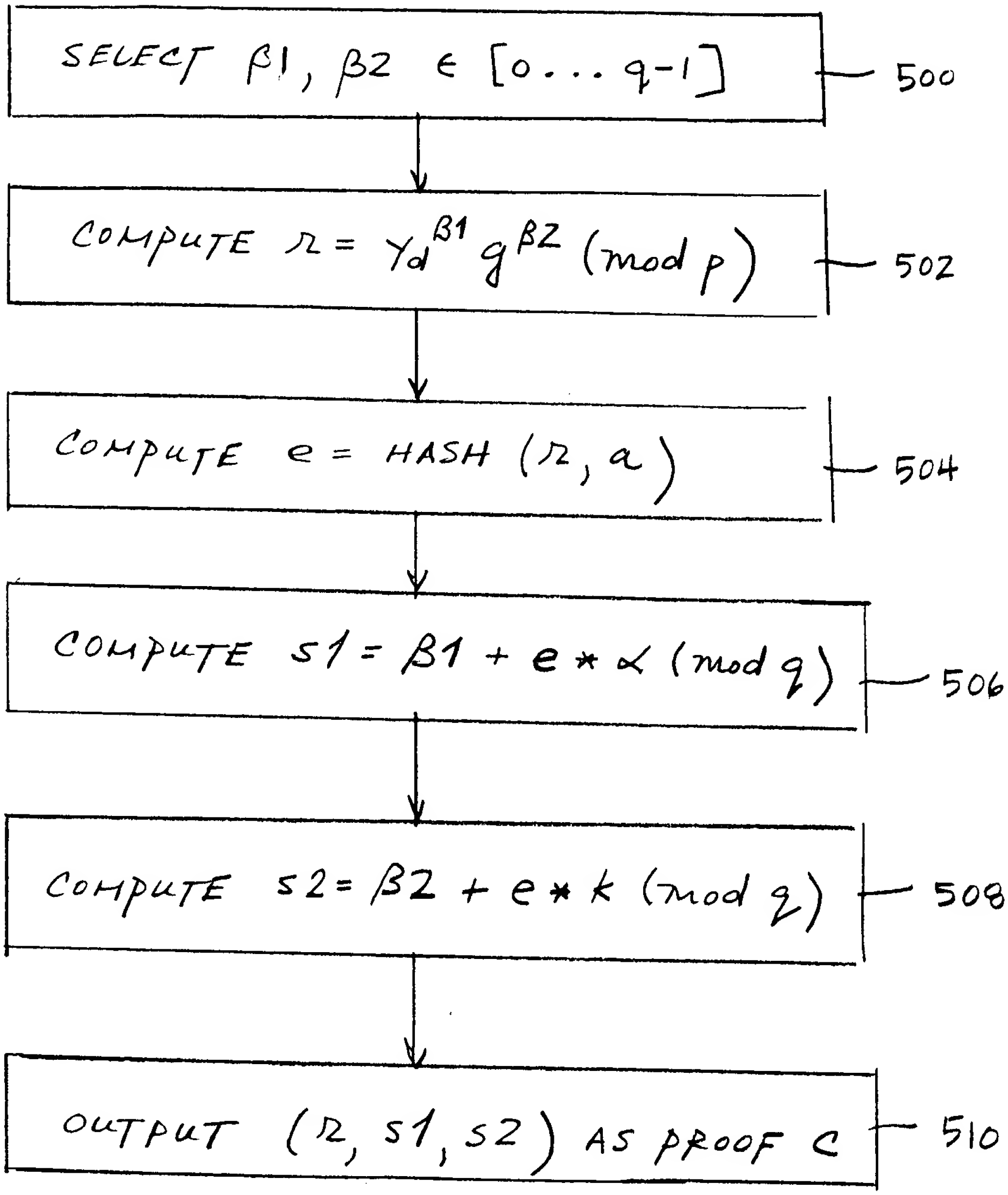
SELECT $\beta 1, \beta 2 \in [0 \ldots q-1]$
500
COMPUTE $r = Y_d^{\beta 1} g^{\beta 2} \pmod{p}$
502
COMPUTE $e = \mathrm{HASH}(r, a)$
504
COMPUTE $s1 = \beta 1 + e * \alpha \pmod{q}$
506
COMPUTE $s2 = \beta 2 + e * k \pmod{q}$
508
OUTPUT $(r, s1, s2)$ AS PROOF c
510

FIG. 5

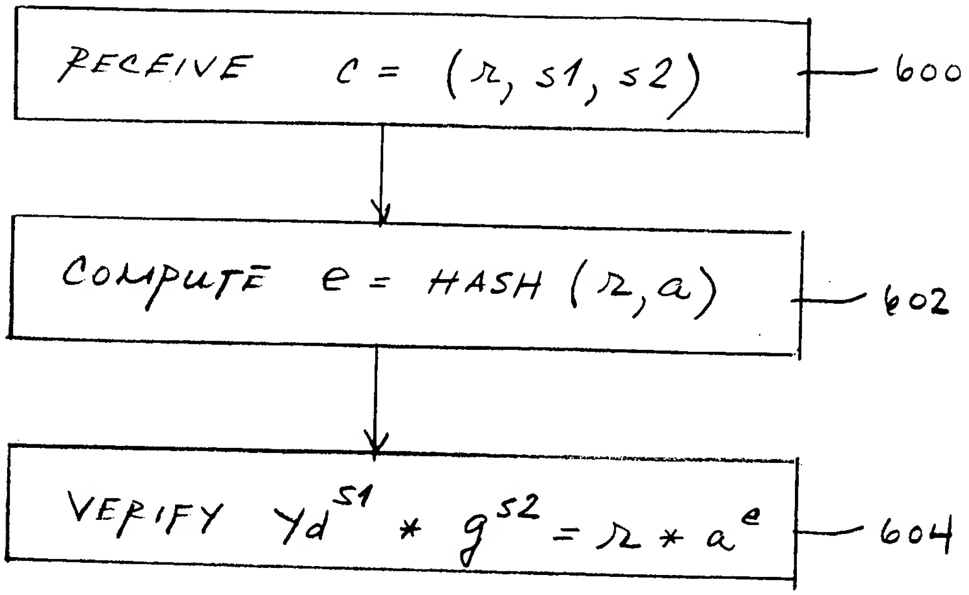
RECEIVE $c = (r, s1, s2)$
600
COMPUTE $e = HASH(r, a)$
602
VERIFY $Yd^{s1} * g^{s2} = r * a^{e}$
604

FIG. 6